S05P0372W000

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2001－521697
（P2001－521697A）
(43)公表日　平成13年11月6日(2001.11.6)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	テーマコード（参考）
Ｈ０４Ｌ　9/18		Ｈ０４Ｌ　9/00	６５１

審査請求　未請求　予備審査請求　有　（全 19 頁）

(21)出願番号　特願平10－544810
(86)（22)出願日　平成10年３月11日(1998.3.11)
(85)翻訳文提出日　平成11年10月21日(1999.10.21)
(86)国際出願番号　ＰＣＴ／ＥＰ９８／０１３９１
(87)国際公開番号　ＷＯ９８／４８５４０
(87)国際公開日　平成10年10月29日(1998.10.29)
(31)優先権主張番号　１９７１６８６１．２
(32)優先日　平成９年４月22日(1997.4.22)
(33)優先権主張国　ドイツ（ＤＥ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＣＮ，ＪＰ，ＫＲ，ＴＲ，ＵＳ

(71)出願人　ドイッチェ　テレコム　アーゲー
ドイツ国．デー―53113　ボン，フリードリヒ―エベルト―アレェ　140
(72)発明者　コワルスキ，ベルント
ドイツ国．デー―57072　ジーゲン，アム　バステンベルグ　4
(72)発明者　ヴォルフェンシュテッター，クラウス―ディーター
ドイツ国．デー―64673　ツヴィンゲンベルグ―ロダウ，ネッカーシュトラッセ　19
(74)代理人　弁理士　岡部　正夫　（外11名）

(54)【発明の名称】　符号化方法および符号化装置

(57)【要約】
本発明は、エンコーダの中に、原価を下げた上、高性能の符号化機能を実現させるための方法および装置について提案するが、このエンコーダは、統合化バーナム暗号を備えたＰＣソフトウェアもしくはその類似装置、またはそのほかの任意な端末機器、情報システムだけから構成され、このバーナム暗号は、本来の符号化プロセスのために、高価な暗号用ハードウェアに支援を求めてはならない。暗号用ハードウェアは、特殊なチップカードが組み込まれたチップカードまたは多機能性ＰＣインタフェース・アダプタ（ＰＣＭＣＩＡモジュール）から構成される。これに対してエンコーダは、従来からのパーソナルコンピュータ（ＰＣ）、ソフトウェアまたは他の端末機器であるが、非常に簡単なバーナム暗号（例えば、ＥＸＯＲ）を、ソフトウェアにおける広帯域用としても使用するほかには、それ以上の暗号技術を必要とするものではない。外部暗号モジュールは、すべて複雑な暗号機能を含み、バーナム符号（ＫＶ）を、いわゆる、貯蔵用として発生させ、これが中間記憶装置に記憶されると、本方法による論理演算子を用いた符号化プロセスに

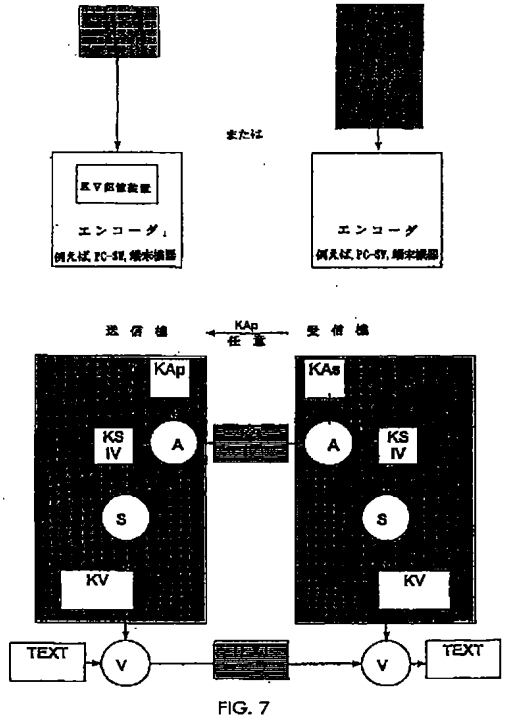


FIG. 7

【特許請求の範囲】

１．符号化プロセス、とくにバーナム暗号を（ここで、符号化方法を、例えば、ＥＸＯＲのような非常に簡単な数学的演算にすることができるが）簡素化して実施するための方法であって、

定義された符号長さ（ｘビット）を有する秘密符号（ＫＳ）の使用により、そして必要な場合には、任意の対称暗号（Ｓ）に関してｎ・ｘの長さのビットを有する可変パラメータ（ＩＶ）の支援により、符号化する通信情報の長さを有するバーナム符号（ＫＶ）が作成され、

バーナム符号（ＫＶ）が、バーナム暗号（Ｖ）の論理演算子を通して保護する通信情報の符号化を行い、

秘密符号（ＫＳ）およびパラメータ（ＩＶ）が、通信情報の伝送路によって分離され、安全化されたチャネルを通して、または直接、通信情報の伝送路において、非対称性方法（Ａ）もしくは類似の方法によって安全化されて、送信機から受信機に伝送され、

受信機が、バーナム符号（ＫＶ）を再生し、そして受信された通信情報の解読を行うことを特徴とする方法。

２．バーナム符号（ＫＶ）のための対称暗号および記憶装置が、エンコーダによって分離された暗号用モジューの中に、チップカード、多機能性ＰＣインタフェース・アダプタまたはモジュール（ＰＣＭＣＩＡ）の形で組み込まれ、

エンコーダの中において、バーナム暗号の演算だけが行われることを特徴とする請求項１記載の方法。

３．バーナム符号（ＫＶ）のための非対称暗号および記憶装置が、エンコーダによって分離された外部暗号用モジュールの中で実際に存在し、

エンコーダの中において、バーナム暗号が、符号化のための演算制御を行うことを特徴とする請求項１記載の方法。

４．エンコーダの中に、バーナム符号（ＫＶ）が記憶されることを特徴とする請求項１－請求項３の何れか１項記載の方法。

５．暗号用ハードウェアが、組み込まれた特殊な暗号用ハードウェアを備えた

チップカードまたは多機能性ＰＣインタフェース・アダプタ（ＰＣＭＣＩＡモジュール）またはその類似装置から構成され、

エンコーダが、従来からのパーソナルコンピュータもしくはその類似装置、ソフトウェアまたは他の端末機器から構成され、ソフトウェアの中に広帯域用に使用する非常に簡単なバーナム暗号を実現させることを特徴とする請求項１－請求項４の何れか１項記載の装置。

６．暗号用ハードウェアが、外部暗号用モジュールとして形成され、そしてバーナム符号（ＫＶ）を貯蔵して記憶するための中間記憶装置をもつことを特徴とする請求項１－請求項４の何れか１項記載の装置。

７．バーナム符号（ＫＶ）を記憶するための記憶装置が、パーソナルコンピュータ（ＰＣ）またはその他の端末機器の中に配置されていることを特徴とする請求項６または請求項７の何れか１項記載の装置。

【発明の詳細な説明】

符号化方法および符号化装置

本発明は、請求項１または請求項５の上位概念に基づく符号化のための方法およびその方法を実施するための装置に関する。

最近の符号化方法は、情報処理および電気通信技術の分野において、ますますその用途を拡大している。しかしながら、符号化方法および相当する装置の使用に関しては、以下に述べるような問題点と影響があるために長い間阻まれているが、一方では、マルチメディアの分野、そして情報処理の領域にまで用途が大幅に拡大している状況において、非常に高い安全性の基準が必要とされる。すなわち、

－広帯域信号を、符号化するためには、パーソナルコンピュータと端末機器の中に高価な暗号用ハードウェアを組み込むことが必要とされる。コストをかけずに使用できる暗号用チップカードは、目下のところ、低い、すなわち明らかに毎秒１００キロビット未満のスループットレートにおいてだけ作動する。

－符号化方法は、保護を受けることが多いために、国際的に標準化されず、その結果、統合化暗号用ハードウェアを備えた製品を、原価を下げ、量産して利用することができない。

－広帯域符号化に使用される暗号用ハードウェアは、コスト面からの理由で、しばしば、ただ１つの符号化方法に利用されるに過ぎない。従って、このようにして装備されたパーソナルコンピュータ、その他の端末機器でも、いくつも存在する符号化方法をサポートしていくことはできない。従って、前記の機器には、その両立性に関して強い制約が生じることになる。

－暗号用ハードウェアは、国際貿易上の厳しい制限を受けるために、例えば、

符号化用の端末機器を輸出することに非常に大きな制約が生じ、そのために、このような装置を使用することが制限されて機器の価額が高騰する。

Ａｌｆｒｅｄ　Ｂｅｕｔｅｌｓｐａｃｈｅｒを著者として、Ｖｉｅｗｅｇ　Ｖｅｒｌａｇ社から出版（１９９３）された著書「Ｋｒｙｐｔｏｌｏｇｉｅ（暗号化技術）」において、例えば、バーナム暗号などの符号化方法について記載と説

明がなされている。その他にも、ＩＴＵ／ＣＣＩＴＴレコメンデーションＸ．５０９、または、ＡＣＭ，Ｖｏｌ．２１，Ｎｏ．２，ｐｐ．１２０－１２６，１９７８の「ＣＡＣＭコミュニケーション」の中で、ＲＳＡ法などの符号化方法について記載されている。

本発明が基にする課題は、符号化ための方法および装置を新規に作り、高価でなく、非両立性を避けた広帯域符号化ハードウェアを実施することを、最も簡素化した方法で実現させて、その結果、統合化暗号用ハードウェアを備え、将来は、原価の低い量産製品を調達して、そして製品の安全性基準を実質的に改良することにある。

本方法を用いた発明による解決は、請求項１の特質において特徴づけられる。

本発明の方法による、その他の解決または形態は、請求項２－請求項４における特質に開示されている。

符号化方法または装置を実施するための解決は、請求項５の特質において特徴づけられる。その他の装置に関する形態は、請求項６および請求項７の特質において特徴づけられている。

本発明による解決方法には大きな長所があり、エンコーダは、同じ種類のバーナム暗号（例えば、ＥＸＯＲ）によって常に作動することができる。このエンコーダは、外部用の暗号モジュールまたはＰＣＭＣＩＡモジュール（多機能性ＰＣインタフェース・アダプタ）が、種々の対称性および非対称性の暗号を扱う

場合でも、問題なく使用することができる。バーナム暗号は、高いスループットレートにおいても、ソフトウェアにおける使用が可能となるために、あらゆるエンコーダは、高価な暗号用ハードウェアを使用しなくて済み、そして製造が技術的に簡単なために、エンコーダの量産を原価を下げて行うことができるようになる。外部暗号モジュールが、同じように原価が低いのは、貯蔵用に生産されるバーナム符号が、低性能または低速のチップカードによって、例えば、バーナム符号の記憶装置に対する貯蔵用として生産されるためであり、このとき減結合的に作動する本来の広帯域符号化プロセスが遅延することがない。

本発明が記載する方法を基にして、エンコーダの性能からは、暗号用ハードウ

ェアのもつ高価性、高性能、そして非両立性の問題点が除去される。これに対してバーナム暗号は、非常に簡素であり、ソフトウェアにおける原価も低いために、記憶装置を用いて実施することができる。すべて複雑な暗号機能は、エンコーダの外部に存在している。この暗号機能は、モジュール的に交換可能であり、本発明が提案する、コストが適切で、低速の外部暗号モジュール、例えば、チップカードまたはＰＣＭＣＩＡカードにおいて実現される。使用する方法については、送信機と受信機の間に同調がなされるときに、例えば、伝送路において取り決められ、または信号化される。エンコーダ自体は、単なるソフトウェア、例えば、統合化バーナム暗号を備えたＰＣソフトウェアまたは他の任意な端末機器／情報システムから構成されて、この暗号は、本来の符号化プロセスとして、高価な暗号用ハードウェアによって支援されなければならないようなものではない。

本発明は、以下に挙げる図において、原理的に表わされた実施例によって詳しく説明される。

図の意味を、以下に記載する。

図１は、簡単に図解した公知のバーナム暗号である。

図２は、最近の公知の対称暗号である。

図３は、非対称暗号を追加して使用した機器構成である。

図４は、バーナム暗号を備えた機器構成である。

図５は、バーナム暗号を備えた他の形式である。

図６は、外部暗号用モジュールを備えた機器構成である。

図７は、暗号用モジュールを備えた他の機器構成である。

図において、以下の説明において、請求項および要約書において使用する参照記号または略語を以下のリストに挙げる。

図１において、バーナム暗号を、簡単に説明する。ここで、Ｖと記した符号化プロセスは、例えば、ＥＸＯＲのような、非常に簡単な数学的演算であり、ここで特殊な暗号用ハードウェアの支援がなくても、ソフトウェアにおける広帯域の符号化をも可能にする。しかしながら、よく知られたこの方法には欠点があり、それは「ＴＥＸＴ」と名付けられた通信情報が、バーナム符号ＫＶを用いて符号

化されなければならず、符号ＫＶが、符号化する通信情報の長さをもつ乱数から構成されることである。従って、長い通信情報には、長いバーナム符号が必要とされる。このためにバーナム暗号を、実際に使用するときには、条件が付けられることである。図２において、例えば、ＤＥＳまたはＩＤＥＡなどの最近の対称暗号Ｓを示すが、この暗号Ｓは、比較的短い長さの符号の場合に、通常の秘密対称暗号ＫＳに対する１２８ビットの場合においても、優れた安全性を示している。ＤＥＳまたはＩＤＥＡは、データ暗号化のスタンダード（ＡＮＳＩまたはＡＳＣＯＭ）、ＩＳＯ　９９７９に記載される。いずれにしてもバーナム暗号の場合のように、ここでも通信情報の伝送路には関係がなく、暗号化および暗号解読に必要とされる秘密符号ＫＳを、安全なチャネルを通して、例えば、クーリエ（Ｋｕｒｉｅｒ）を介して交換しなければならない。図３に示す機器構成については、本明細書の初めに挙げた文献で詳しく説明されるが、暗号用の秘密符号ＫＳを伝送するために、例えば、ＲＳＡ方法に非対称性の暗号Ａを追加して使用することによって、機器構成の欠点を取り除いた。このとき符号化符号ＫＳは、受信機ＫＡｐの公開された非対称符号によって符号化され、引き続いて秘密対称暗号を用いて再び解読することができる。この目的のために送信機で必要とされる公開の受信機符号ＫＡｐは、任意の安全性のないチャネルを通じて受信機から送信機に伝送される。通信情報を、公開の受信機符号ＫＡｐによって直接的に符号化することも勿論のこと可能ではあるが、非対称暗号として使用されるハードウェアおよびソフトウェアについて得られた性能が、対称暗号の場合と比較して明らかに低いために、通信情報が長い場合には、処理速度を高めるために、多くの場合、非対称暗号と対称暗号を、図３のように組み合わせて、つまりハイブリッド方式をとって使用する。図４において示されるが、可変長さをもつ、例えば、ｎ・１８０ビットの秘密パラメータＪＶの符号化を、例えば、１２８ビットの対称暗号ＫＳを用いて行うことによって、非常に長い（疑似）乱数が発生し、これが最終的にバーナム符号ＫＶとして、保護すべき通信情報を符号化する。受信機側において暗号符号および解読符号を伝送するために、クーリエは、バーナム符号ＫＶを運ぶ必要はなく、単に符号ＫＳとパラメータＩＶを運ぶことによって、

バーナム符号ＫＶが、簡単に受信機側に形成されるが、これは送信機側と同じような機器構成が、受信機側にも存在するからである。図５においては、図４と同じように非対称暗号、対称暗号およびバーナム暗号の組み合わせによる符号化が示される。秘密符号情報の交換のために、クーリエを必要とする図４とは反対に、図５においては、図３と同じく非対称暗号が使用される。送信機側には、公開の受信機符号ＫＰａが供給され、受信機側には、非対称性の送信機符号ＫＡｐが供給される。

この方式の長所は、図７および図８において明らかにされる。それぞれ図６および図７の上半分に、典型的な２つの端末機器の機器構成が図示される。グレイに裏打ちされている箇所は、特殊な暗号用ハードウェアまたは特殊なチップカードが組み込まれたチップカードまたは多機能性ＰＣインタフェース・アダプタもしくはＰＣＭＣＩＡモジュールから構成される外部暗号用ハードウェアを表わしている。これに対してエンコーダは、ソフトウェアまたはその他の端末機器を備えた従来のＰＣとして実用されるが、例えば、ＥＸＯＲのように非常に簡素化されて、ソフトウェアにおいて広帯域用としても使用されるバーナム暗号のほかには、何らの暗号技術を必要とするものではない。図６および図７のいずれにも示されるように、外部暗号モジュールは、すべて複雑な暗号機能を取り込むことができ、バーナム符号ＫＶを、いわゆる貯蔵用として発生させ、これが適切な中間記憶装置、ＫＶ装置に入力されると、論理演算子Ｖによる符号化プロセスにおいて少しずつ消費される。このときＫＶ記憶装置を、パーソナルコンピュータまたは端末機器にも、そして暗号モジュールにも、チップカードまたはＰＣＭＣＩＡモジュールの形で組み込むことができる。図６および図７に示す装置の長所として挙げられるように、外部暗号モジュールまたは外部ＰＣＭＣＩＡモジュールが、異種の対称暗号および非対称暗号を扱ったとしても、このエンコーダは、常に同種のバーナム暗号を用いて作動することができる。バーナム暗号は、ソフトウェアにおいて高いスループットレートによっても実用することができるので、エンコーダは、すべて高価な暗号用ハードウェアを使用しないで、量産的に原価を下げて製造することができる。同様に外部暗号用モジュールが、原価を下げられ

るのは、貯蔵用に生産されるバーナム符号が、低性能、つまり低速のチップカードによってＫＶ記憶装置の貯蔵用として作られるからであり、そのために減結合的に作動する、本来の広帯域符号化プロセスが、低速化されることはない。

記載した方法に基づくと、前記エンコーダから、暗号用ハードウェアが有する高価、高性能、そして相互間の非両立性の問題点が、取り除かれる。これに対してバーナム暗号は、ソフトウェアにおいて非常に簡単に、原価を下げて実用化される。あらゆる複雑な暗号用機能は、エンコーダの外に存在する。大きな長所がさらに存在し、機能は、モジュール的に交換可能であり、今回提案のコストを要しない、低速の外部暗号用モジュール、例えば、チップカードまたはＰＣＭＣＩＡカードにおいて実現が可能である。使用する方法は、送信機と受信機の間の同調で、例えば、伝送路において取り決められ、または信号化される。

統合化バーナム暗号を備えたＰＣソフトウェアまたはそのほかの任意な端末機器、情報システムだけから構成され、このバーナム暗号が、本来の符号化プロセスのために高価な暗号用ハードウェアの支援を求めてはならないエンコーダに対し、原価の低い高性能の符号化機能を実現させる方法の特徴として、以下に記すように定義された符号長さを有する秘密符号ＫＳを用い、そして任意の対称暗号Ｓに関して定められたビット長さを有する可変パラメータに支援されて、符号化される通信情報の長さを有するバーナム符号ＫＶが作成され、この通信情報からバーナム暗号を通して保護すべき通信情報が符号化されて、ここで秘密符号ＫＳおよびパラメータＩＶが、通信情報の伝送路によって分離、安全化されたチャネルを通じてか、または通信情報の伝送路において直接的に、例えば、非対称性方法Ａによって安全化されて送信機から受信機に伝送され、このとき後者であるパラメータＩＶが、上述の方法によってバーナム符号ＫＶを再生して、受信された通信情報の解読が可能になるようにすることが挙げられる。必要な場合には、非対称暗号をも含む対称暗号が、そして必要な場合には、バーナム符号のための記憶装置が、すなわち、ＫＶ記憶装置が、エンコーダによって分離された外部暗号用モジュールの中に、例えば、チップカードまたはＰＣＭＣＩＡカードまたは類

似の形で組み込まれ、そしてエンコーダの中には、バーナム暗号、必要な場合には、バーナム符号のための記憶装置ＫＶだけが残る。

＜参照記号のリスト＞

ＫＶ	バーナム符号
Ｖ	論理演算子、例えば、ＥＸＯＲ
ＫＳ	秘密対称符号
Ｓ	対称暗号、例えば、ＩＤＥＡ
ＫＡｐ	受信機符号（非対称性）
ＫＡｓ	送信機符号（非対称性）
Ａ	非対称暗号
ＩＶ	秘密可変パラメータ
ＰＣＭＣＩＡ	多機能性ＰＣインタフェース・アダプタ
ＰＣ－ＳＷ	ＰＣソフトウェア

【図１】

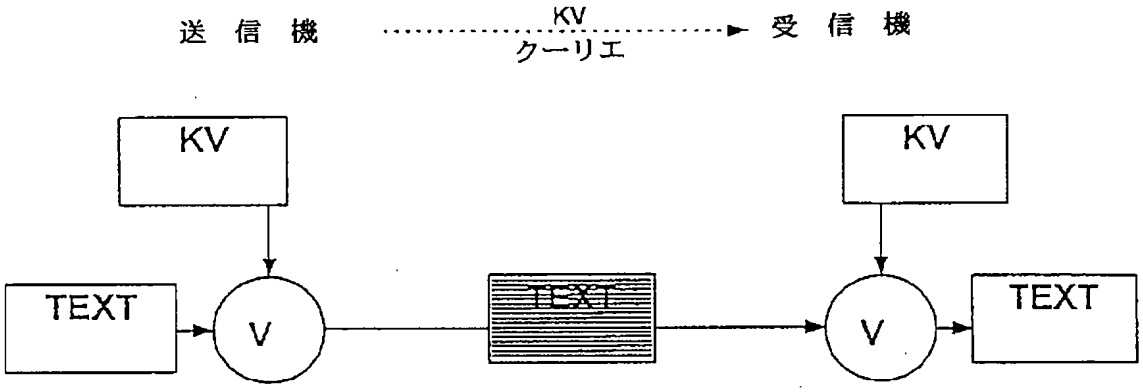


FIG. 1

【図２】

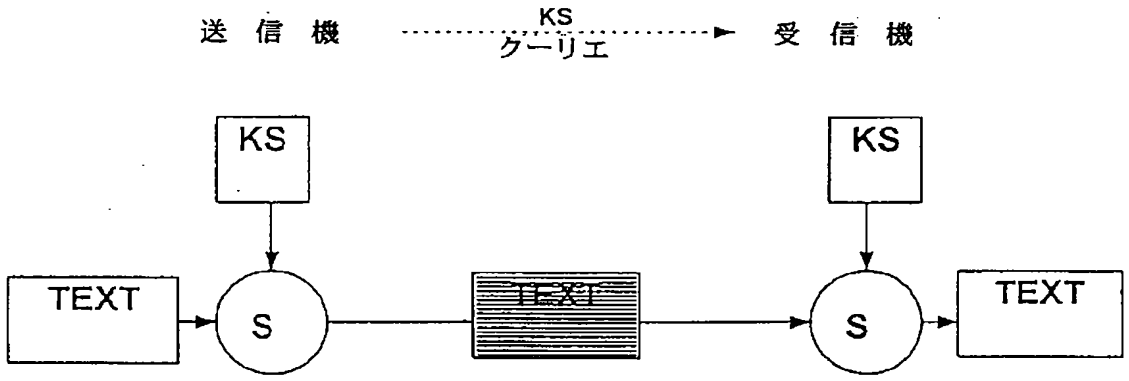


FIG. 2

【図３】

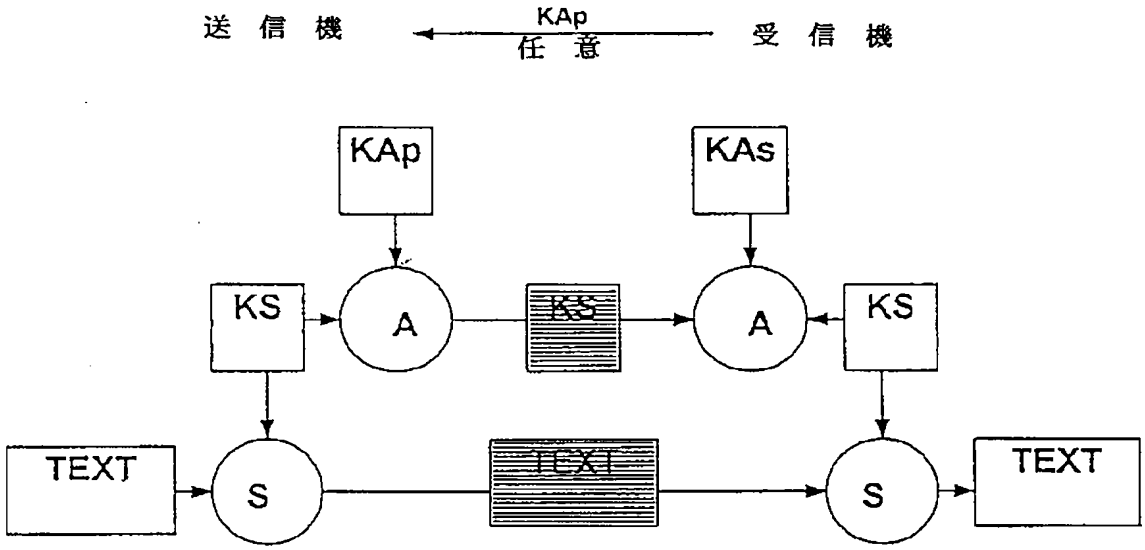


FIG. 3

【図４】

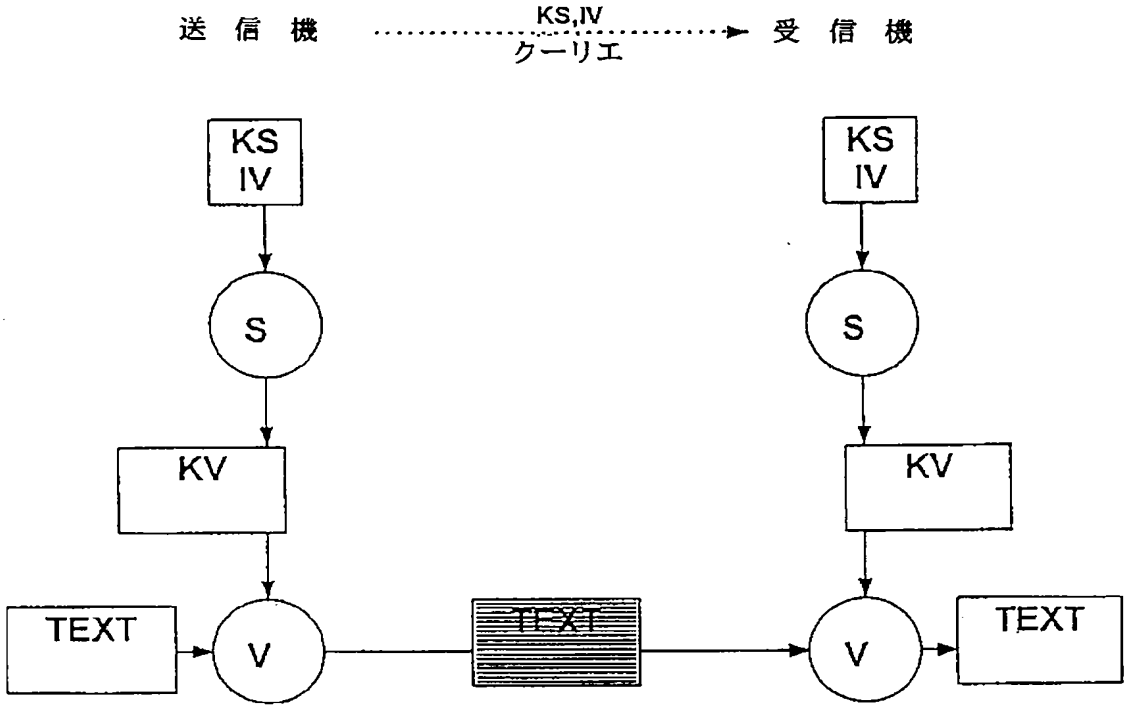


FIG. 4

【図５】

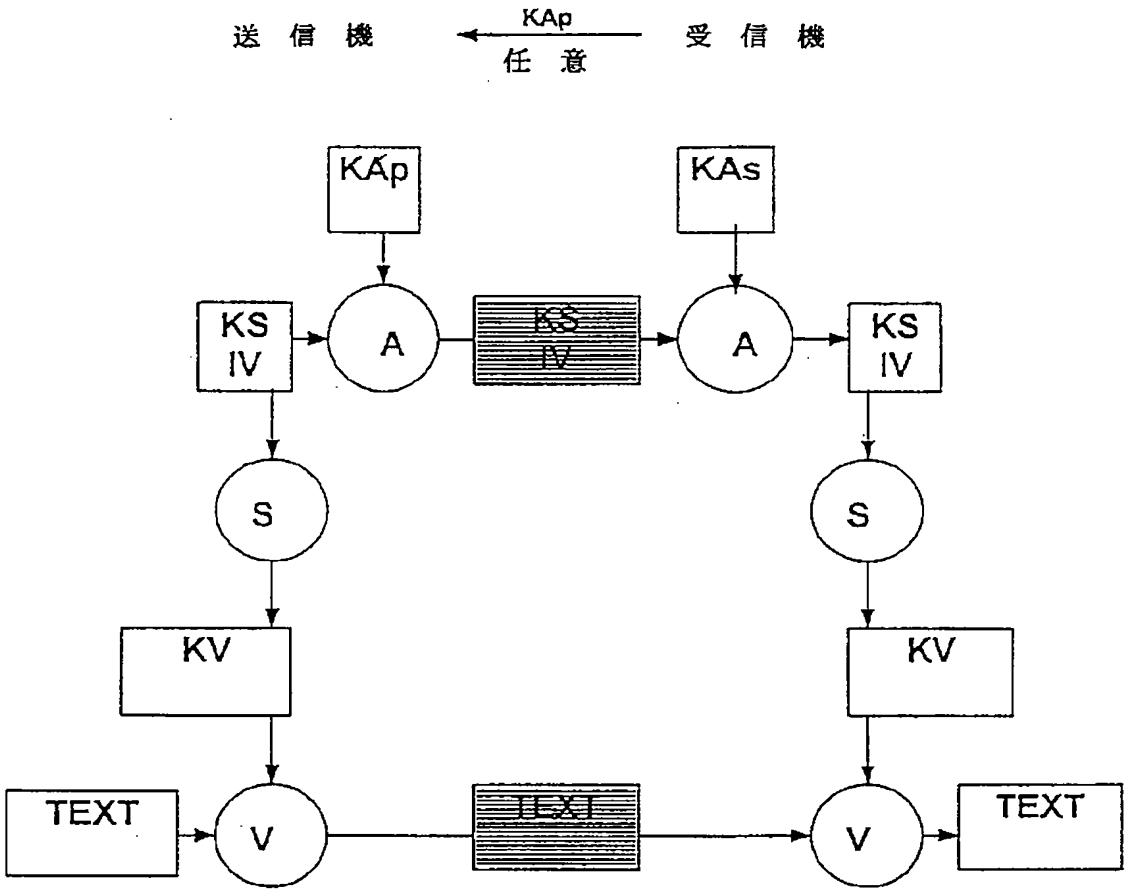

送信機
KAp
任意
受信機
KAp
KAs
KS IV
A
KS IV
A
KS IV
S
S
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 5

【図６】

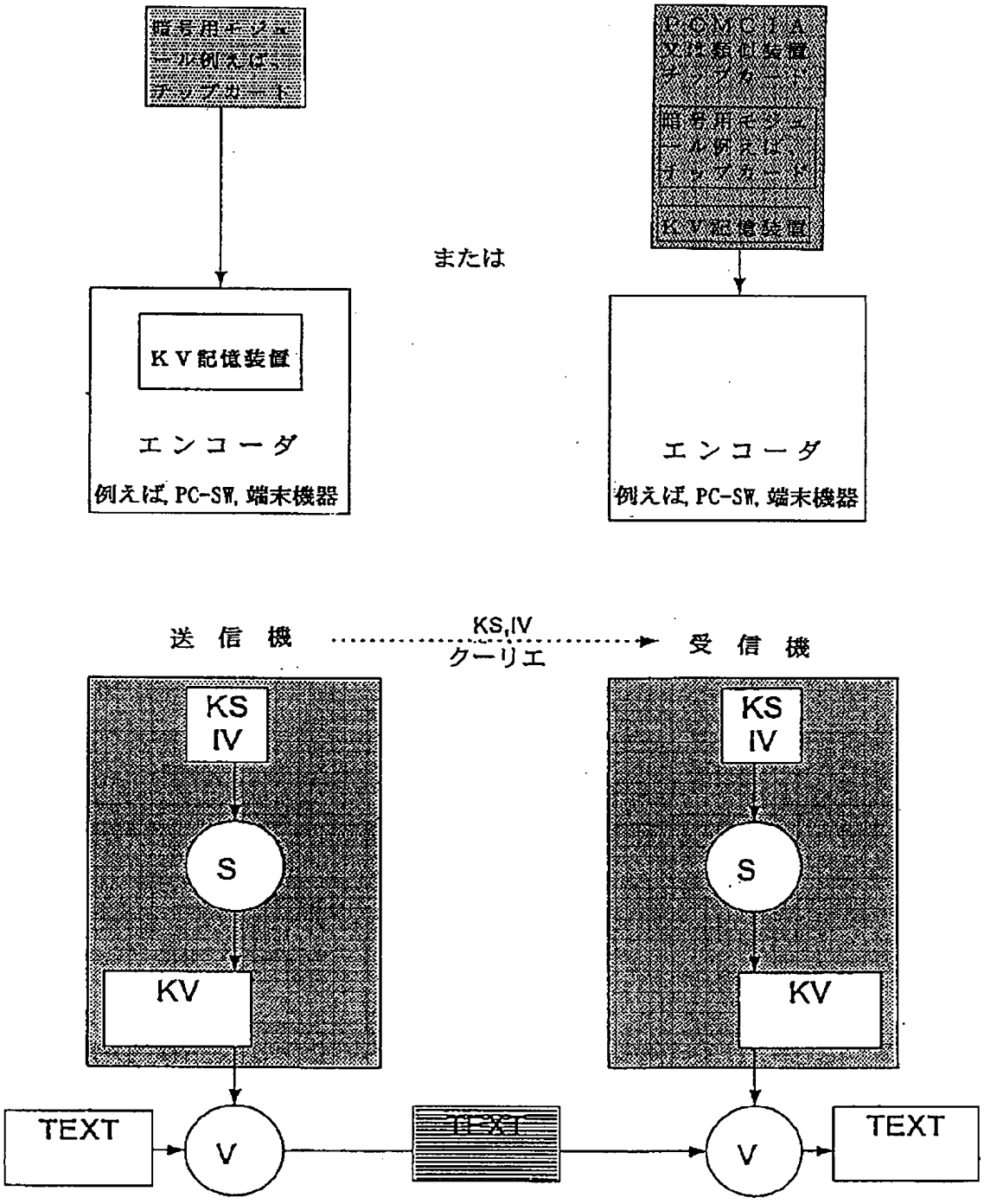
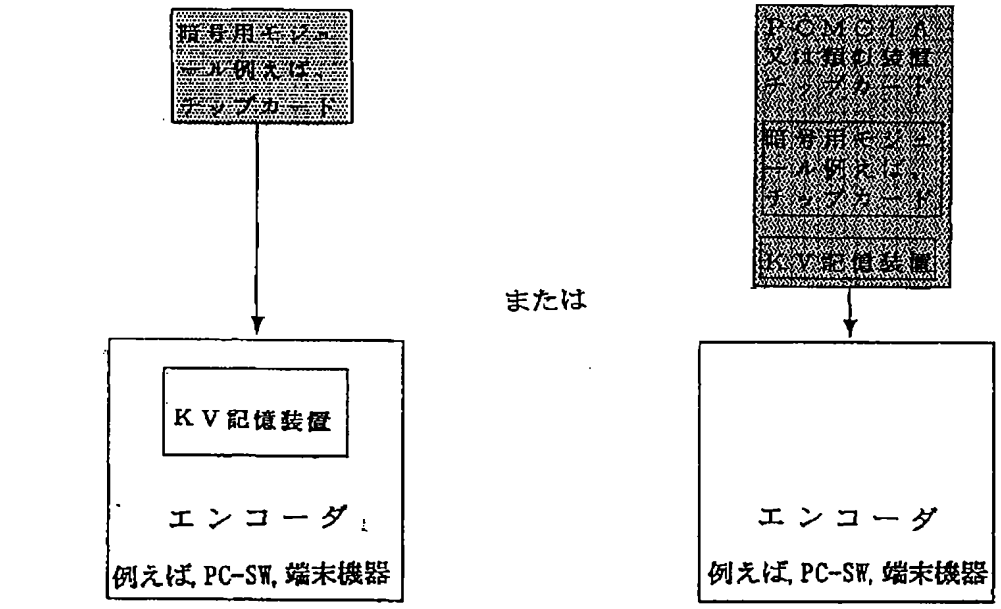

暗号用モジュール例えば、チップカード
KV記憶装置
エンコーダ
例えば、PC-SW、端末機器
または
PCMCIAまたは類似装置チップカード
暗号用モジュール例えばチップカード
KV記憶装置
エンコーダ
例えば、PC-SW、端末機器
送信機
KS,IV
クーリエ
受信機
KS
IV
S
KV
TEXT
V
TEXT
KS
IV
S
KV
V
TEXT

FIG. 6

【図７】


指令用モジュール例えば、チップカード
KV記憶装置
エンコーダ
例えば、PC-SW、端末機器
または
PCMCIAまたは指令装置チップカード
指令用モジュール例えば、チップカード
KV記憶装置
エンコーダ
例えば、PC-SW、端末機器

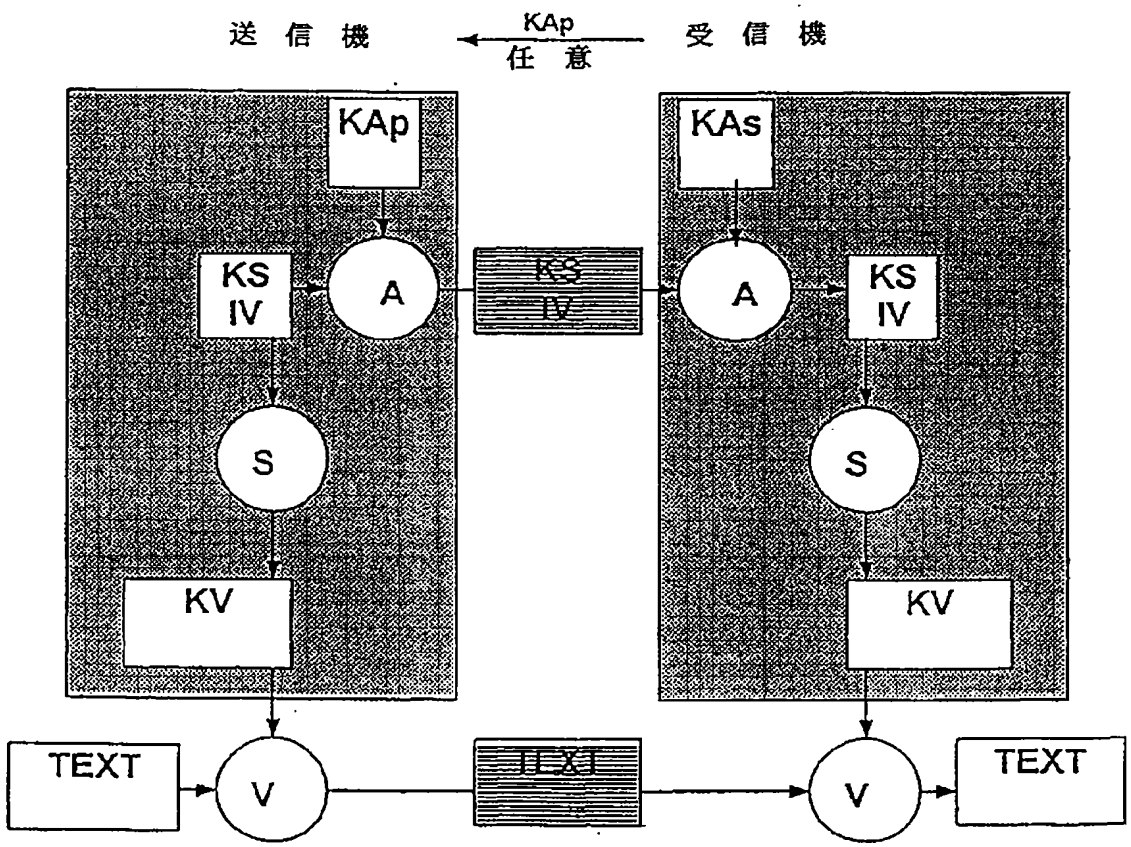

送信機
KAp
任意
受信機
KAp
KAs
KS IV
A
KS IV
A
KS IV
S
S
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 7

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 98/01391

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/18 G07F7/10

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FEY P: "VERSCHLUESSELUNG VON SPRACHE UND DATEN" NACHRICHTENTECHNIK ELEKTRONIK, vol. 40, no. 10, 1 January 1990, pages 376-377, XP000176445 BERLIN (DE)	1
Y	see page 376, right-hand column, last paragraph - page 377, right-hand column, last line	2
A	DE 27 06 421 B (LICENTIA) 29 June 1978 see column 3, line 61 - column 5, line 28	1
Y	EP 0 616 429 A (SIEMENS) 21 September 1994	2
A	see column 1, line 28 - line 50 see column 3, line 38 - column 4, line 11	5,6

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 September 1998	08/09/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 98/01391

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 974 193 A (BEUTELSPACHER ETAL.) 27 November 1990 see column 2, line 49 - column 3, line 41	2
A	US 5 513 261 A (MAHER) 30 April 1996 see column 2, line 27 - line 62 see column 3, line 16 - line 21	2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 98/01391

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
DE 2706421	B	29-06-1978	AT	376344 B	12-11-1984
			AT	87678 A	15-03-1984
			CH	639229 A	31-10-1983
			FR	2381423 A	15-09-1978
			GB	1598415 A	23-09-1981
			NL	7801619 A	18-08-1978
			US	4211891 A	08-07-1980
EP 616429	A	21-09-1994	JP	6244684 A	02-09-1994
US 4974193	A	27-11-1990	DE	3706955 A	15-09-1988
			DE	3889481 D	16-06-1994
			EP	0281057 A	07-09-1988
			ES	2051780 T	01-07-1994
			JP	63228353 A	22-09-1988
US 5513261	A	30-04-1996	NONE		

【要約の続き】
おいて少しずつ消費される。このとき記憶装置を、ＰＣまたは端末機器にも、そして暗号モジュールにも組み込むことができる。外部暗号モジュールまたは外部ＰＣＭＣＩＡモジュールが、異種の対称暗号および非対称暗号を使用したとしても、このエンコーダは、常に同種のバーナム暗号によって作動することができる。外部バーナム暗号は、チップカードまたはＰＣＭＣＩＡモジュールの形をとって原価を下げて製造することができる。複雑な暗号用機能は、すべてエンコーダの外に置かれる。この暗号用機能は、モジュール的に交換可能であり、本発明の提案により、コストを要せず、多少低速の暗号用モジュールの中において実現される。